Security Advisory

8/2/2001
Revision 2.0

It has come to our attention that web servers within the KETS environment have various vulnerabilities that can lead to a breach of security. These breaches of security can lead to web site defacements, access to sensitive data and denial of service attacks. This document details steps for securing Microsoft NT 4.0 Servers. We recommend reading this document very carefully and taking all recommended actions immediately for **every** Microsoft NT 4.0 Server.

Determining Service Pack Level for Windows NT 4.0 Servers

Windows NT 4.0 Service Pack 6a is required for installation of the hotfixes discussed in this security advisory. To check your server for the service pack level, follow the steps listed below:

1. Click Start -> Run
2. Type 'winver'
3. Press 'Enter'

If the 'About Windows NT' box states:

Microsoft(R) Windows NT (R)
Version 4.0 (Build 1381: Service Pack 5)
Copyright (C) 1981-1996 Microsoft Corp

The system is running SP5.

If the 'About Windows NT' box states:

Microsoft(R) Windows NT (R)
Version 4.0 (Build 1381: Service Pack 6)
Copyright (C) 1981-1996 Microsoft Corp

The system is running SP6.

If the 'About Windows NT' box states:

Microsoft(R) Windows NT (R)
Version 4.0 (Build 1381: Service Pack 6)
Copyright (C) 1981-1996 Microsoft Corp
Revised Service Pack 6a

The system is running SP6a.

If Service Pack 6a is already installed on your server proceed to the ***Determining Internet Information Services Version*** instructions. If Service Pack 6a is not installed on your server proceed to the download and installation instructions for Microsoft NT Service Pack 6a.

Download and Installation Instructions for Microsoft NT Service Pack 6a

1. Click the link http://www.kde.state.ky.us/oet/system/proxy/downloads/msnt128.exe
2. Click 'save program to disk'
3. Save the 'msnt128.exe' file to the desktop
4. Double-click the 'msnt128' file

NOTE: Make sure to check 'Back up files necessary to uninstall this Service Pack at a later time (requires approximately 60MB additional disk space)'

5. Follow the instructions that are listed in the window

NOTE: SP6a installation will not be completed until you reboot your computer.

Determining Internet Information Services Version

To identify what version of IIS is currently installed on your server:

1. Start the Microsoft Management Console
2. Click the 'Help' menu
3. Click 'About'

A window will be displayed which shows the version number. If you do not have IIS 4.0 installed on your computer, download and install IIS 4.0 from http://www.microsoft.com/ntserver/nts/downloads/recommended/NT4OptPk/default.asp.

If updates were made in this section you must re-apply Service Pack 6a

Determining Internet Explorer Version

All servers must have Microsoft Internet Explorer 5.5 with Service Pack 2.0 installed on the computer. To determine which version of Internet Explorer is running on a computer:

1. Start Internet Explorer
2. Click the "Help" Menu
3. Click "About"

A window will appear and display what version of Internet Explorer is installed on the machine.

If you are not running Internet Explorer 5.5 with Service Pack 2.0, download it from http://www.microsoft.com/windows/ie/download/ie55sp2.htm

If updates were made in this section you must re-apply Service Pack 6a

Determining Proxy Server Service Pack Level

All servers running Microsoft Proxy Server must running Proxy Server 2.0 and have Proxy Server Service Pack 1 installed. If Proxy Server SP1 isn't installed, you must first download and install it on your server. To check to see if Service Pack 1 is installed:

1. Start the Microsoft Management Console

2. Right Click the 'Microsoft Proxy Server'
3. Click 'Properties'

A popup screen will appear and display what version of Proxy Server and service pack is installed.

If you are not running Microsoft Proxy Server SP1, you can download it from
http://www.kde.state.ky.us/oet/system/proxy/downloads/msp2sp1i.exe .

If updates were made in this section you must re-apply Service Pack 6a

Determining SMS Service Pack Level

All servers running Microsoft SMS must running version 2.0 and have SMS Service Pack 3 installed. If SP3 for Microsoft SMS 2.0 isn't installed on the server you must first download and install it on your server. To check to see if SP3 is installed on your SMS server:

1. Click Start -> Programs -> System Management Server -> SMS Administrator Console
2. Right Click the 'Site Database'
3. Click 'About'

A popup screen will appear and display what version of SMS / Service Pack is installed

These products can be downloaded from
http://www.microsoft.com/smsmgmt/default.asp

If updates were made in this section you must re-apply Service Pack 6a

Special Instructions for Microsoft Exchange Servers

All servers running Microsoft Exchange must disable the Exchange Information Store before installing the hotfixes.

Special Instructions for Servers Running Anti-Virus Software

Disable all anti-virus software (Net Shield, Group Shield, Trend, Norton, etc.) prior to running this script and make sure it is set to be disabled on reboot.

Download and Install instructions for Microsoft NT 4.0 Server Post Service Pack 6a Security Rollup Package

Once all of the above requirements have been satisfied, the Microsoft Post Service Pack 6a Security Rollup Package **MUST** be applied. You should take every precaution while installing these on your system including doing a **full system backup** before continuing.

* While this utility was tested both by Microsoft and the Kentucky Department of Education, it was not tested on every possible combination of hardware and software that could be installed on your system. Therefore before you begin any of these processes it is recommended that a full system backup be done and completely tested.

This can be downloaded from
http://www.microsoft.com/downloads/release.asp?ReleaseID=31240

Download and Install instructions for Microsoft Security Bulletin MS01-033 (CODE RED PATCH)

Once the Post Service Pack 6a Security Rollup Package has been applied the Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise (*CODE RED PATCH*) **MUST** be applied.

This can be downloaded from
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp

If you have any questions beyond the scope of this document, please contact the KETS helpdesk at 866-KETS-HELP. They can provide you assistance with any questions or problems you may have concerning proxy server security configuration options.

All security advisories will be adopted as KETS technical standards in networking, proxy, and messaging. During the advisory period, comments can be sent to the KETS Security Advisory e-mail address at KETSSecurityAdvisory@kde.state.ky.us.

KETS STANDARDS ADOPTION DATE: 8/02/2001